Cassandra Crossing 625/ Tracciamento delle Notifiche: ultima frontiera

(625)—I sistemi di tracciamento massivo evolvono: dai dati di cella al geofencing degli IP fino al tracciamento delle notifiche push.

Cassandra Crossing 625/ Tracciamento delle Notifiche: ultima frontiera



Figure 1:

(625)—I sistemi di tracciamento massivo evolvono: dai dati di cella al geofencing degli IP fino al tracciamento delle notifiche push.

13 giugno 2025—Cassandra ve lo dice da decenni; la storia del tecnocontrollo sociale è piena di casi di successo.

Vale solo la pena di ricordare la "potenza di fuoco" degli ormai vetusti dati di cella GSM per la localizzazione di qualsiasi possessore di telefono cellulare, che ha dato inizio, anche dal punto di vista legislativo, ad un tecnocontrollo di Stato sulla posizione, anche storicizzata, dei propri cittadini possessori di un telefono cellulare.

La potenza di questo armamentario è aumentata a dismisura non appena i cellulari GSM si sono trasformati in smartphone, e la loro connessione ad Internet è divenuta regola invece di eccezione, grazie alla drastica diminuzione, anzi al quasi azzeramento dei costi della connessione internet per gli utenti.

Questo ha permesso di incrociare i dati di cella GSM con i dati di connessione wifi e traffico a livello TCP/IP, aumentando sia la quantità che la precisione dei dati che qualsiasi smartphone rende disponibili ai fini di un controllo centralizzato.

Anche la precisione della posizione è aumentata di molto, grazie all'utilizzo della modalità di localizzazione precisa che gli smartphone possiedono, tramite l'utilizzo delle reti wifi a cui lo smartphone stesso si aggancia.

Questa precisione ha reso disponibili nuove modalità di intercettazione di massa, correntemente utilizzate in varie democrazie compiute e non; un esempio per tutti il geofencing applicato ad un evento nel tempo e nello spazio.

Infatti, grazie alla storicizzazione dei dati di cella GSM e soprattutto della localizzazione precisa dei cellulari tramite le reti wifi agganciate, informazione condivisa con tutte le app ed i servizi dal sistema operativo dello smartphone, è possibile realizzare quello che viene chiamato "**geofencing**".

Si tratta semplicemente di richiedere, tramite il database storico delle posizioni, non i dati di un singolo cellulare, ma di sapere quali sono tutti i cellulari che erano attivi in un certo rettangolo dello spazio ed in un certo intervallo di tempo.

Anche se questo potrebbe apparire persino desiderabile in certe situazioni estreme, il semplice fatto che sia possibile apre a devastanti possibilità di tecnocontrollo sociale e profilazione continui ed oppressivi, quali il sapere esattamente a distanza di anni chi si trovava ad una certa riunione od in una certa manifestazione. Questo tipo di indagine dovrebbe essere esclusa a priori, e **normata con la stessa cura, anzi con cura anche maggiore, di quella riservata all'uso dei captatori informatici**.

Già, i captatori informatici. Molti non hanno ben presente cosa ha significato, per la facilità, l'economia e le potenzialità delle indagini, la diffusione capillare degli smartphone.

Oggi la complessità ed il costo di una perquisizione informatica o di una intercettazione ambientale nei confronti di una persona si sono grandemente ridotti, proprio perché possono essere svolti tramite il cellulare che molto opportunamente chiunque porta sempre con sé.

Ecco perché la regolamentazione delle intercettazioni e delle perquisizioni mediante captatori telematici deve essere normata e limitata in maniera estremamente accurata per evitare eccessi, abusi ed usi illegali.

Ma questa situazione di "vantaggio" per gli investigatori si è ulteriormente incrementata negli ultimi anni. Infatti il proliferare delle app rende possibile un ulteriore aumento delle possibilità di tracciamento sia in tempo reale che storicizzato, e addirittura di interazione diretta con l'indagato, senza l'impiego di captatori informatici installati sullo smartphone.

Vediamo come. Tutte le app, per necessità o per comodità dell'utente, possiedono le "famigerate" notifiche. Si tratta della ricezione continua, in modalità push, cioè non richiesta dall'utente ma subita dallo stesso. E sono "famigerate" non solo per il disturbo che arrecano, ma anche per le possibilità di uso ai fini di tecnocontrollo.

Ricevere una notifica per un evento su un app richiede la realizzazione di un sistema abbastanza complesso, che in questa sede è possibile descrivere solo per sommi capi.

Innanzitutto il gestore della app deve realizzare un server che possa ricevere e memorizzare la richiesta di una particolare copia della app installata in un certo smartphone, il cui proprietario vuole ricevere una notifica.

Viene allora generato un token, che contiene un identificativo univoco del particolare smartphone e della particolare app ivi installata, che viene inviato al server delle notifiche, il quale lo memorizza permanentemente.

Da quel momento, il server delle notifiche, che è anche in possesso di un modo per raggiungere via rete lo smartphone, può contattare in ogni momento il particolare smartphone, per fargli obbligatoriamente consegnare ad una particolare app un particolare messaggio. Questo può sembrare relativamente innocuo, ma lasciate che Cassandra prosegua.

Per motivi di praticità, i produttori di sistemi operativi (Apple, Google, etc.) mettono a disposizione un servizio centralizzato e "gratuito" per la gestione delle notifiche, a cui il gestore di ogni app può collegarsi senza bisogno di avere un proprio server. Ovviamente la "convenienza" è tale che quasi tutte le app lo utilizzano.

Un maligno potrebbe pensare che i produttori dei sistemi operativi lo facciano per memorizzare ancora più dati degli utenti per trarne profitto, ma questa è ovviamente una malignità degna solo di Cassandra, e che qui non verrà ulteriormente discussa.

Bene, cosa succede a questo punto?

Innanzitutto l'utente che ha scelto di ricevere una particolare notifica **ha compiuto una scelta irreversibile**. Infatti è vero che in ogni momento può sospendere le notifiche, ma il processo di generazione e memorizzazione del token da parte del gestore delle notifiche non viene annullato.

Le notifiche quindi continueranno ad essere consegnate al servizio che gira in background sul particolare smartphone, e semplicemente quest'ultimo non le consegnerà alla app, oppure quest'ultima le scarterà senza mostrarle all'utente.

Il nuovo tracciamento così iniziato, quindi, non cesserà mai; l'utente non ha più la possibilità di sottrarsi. Pensateci, quando installate una nuova app. Se la questione vi preoccupa, dovreste disabilitare le notifiche dalla nuova app senza prima aprirla. Si può fare facilmente dalle impostazioni.

Ma se non lo avete fatto, dalla installazione della app in poi la memorizzazione storica dei token del particolare smartphone e delle varie consegne di notifiche al particolare smartphone permetterà, in teoria, le stesse operazioni di tracciamento possibili con i dati di cella GSM e di tracciamento della posizione via indirizzo IP, ovviamente "potenziato" dal wifi.

E questa nuova **modalità avrà una flessibilità ed una granularità infinitamente superiori**, potendo selezionare in massa gli utenti, non solo con operazioni simili al geofencing, ma basandosi su molte più informazioni, a cominciare da quali app sono installate e quando se ne fa o se ne è fatto uso.

Pensate ad esempio alle donne che usano una app per il rilevamento del ciclo, e si spostano da uno stato che consente l'interruzione di gravidanza ad un altro che la persegue come reato. Quando avrete ben considerato le possibili conseguenze, già realizzatesi, di questa situazione, **moltiplicatela all'infinito per tutte le cose che fate con una qualsiasi app tra le centinaia che avete installato sul vostro smartphone**. Traetene infine le vostre conclusioni personali.

Ma c'è ancora di più.

In generale le app di messaggistica permettono di ricevere notifiche quando arriva un nuovo messaggio da un certo mittente o da una certa chat. Questo può essere fatto in vari modi, ma la potenzialità di questo fatto appare evidente e non necessita di ulteriori spiegazioni.

Qualcuno tra i 24 informatissimi lettori obbietterà ora che esistono app di messaggistica che consentono, grazie alla crittografia, di nascondere non solo il contenuto del messaggio, ma anche i suoi metadati.

Vero, ma neppure queste sono immuni dal tracciamento mediante notifiche, perché il tracciamento delle notifiche, se è stato abilitato anche solo una volta, ormai colpirà anche loro fintanto che il cellulare non verrà dismesso.

Qui i dettagli si complicano, ma intanto, se è disponibile il token dell'applicazione sul server delle notifiche, è possibile tracciare un profilo temporale delle notifiche stesse, e quindi determinare cosa stava facendo l'utente in particolari momenti.

Ma c'è di più. Il gestore del server di notifiche, direttamente o su richiesta dall'autorità giudiziaria, può in un determinato istante inviare una "falsa" notifica ad una app di un determinato smartphone, per controllare dove si trovi in quel preciso momento lo smartphone stesso, oppure in certi casi se l'utente sta partecipando ad una particolare chat.

Fin dal 2017 sono stati riferiti casi, raramente riportati dalla stampa statunitense, in cui l'FBI ha fatto uso di queste tecniche, ovviamente senza ricorrere a nessun warrant, poiché nulla è stato normato per questi particolari dati. La questione è poi esplosa sui media nel 2023, quando il senatore statunitense Ron Wyden ha scritto e pubblicato una lettera al Dipartimento di Giustizia che denunciava questo uso.

Viene perciò da chiedersi quanto possano essere diffusi oggi questi utilizzi investigativi, e quanto l'impiego di tecniche che potremmo battezzare di **"app-fencing"** sia correntemente utilizzato da attori vari, senza nessuna autorizzazione o tutela da parte della legge e delle autorità giudiziarie per i cittadini-utenti.

Concludendo; **si è aperto un mondo nuovo, ed ancora poco conosciuto, per il tecnocontrollo** a scopi commerciali, di indagine e di controllo sociale, sia legali che illegali.

A Cassandra, ed a tutti noi che non possiamo diventare *"eremiti digitali"*, rimane solo **la speranza che i legislatori ed i Garanti per la Protezione dei Dati Personali si attivino presto, e facciano anche un buon lavoro**.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

Licenza d'utilizzo*: i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.

By Marco A. L. Calamari on June 20, 2025.

Canonical link

Exported from Medium on August 27, 2025.